

 <b>Information and Communications Technology Division</b>	<b>Guideline</b>	
	<b>Effective Date</b>	<b>Date of Last Revision</b>
	August 2, 2005	August 18, 2005
<b>Chapter Name</b>	<b>Chapter Number</b>	
8.0 SECURITY	8.1 G	
<b>Title</b>		
8.1 G Password Creation Guidelines		

### 1.0 Purpose

The purpose of these guidelines is to provide information for choosing an acceptable password that is difficult for a person, or automated system, to gain access to by guessing or otherwise deducing a user password—either by a one-time random act or by systematic brute force attack.

### 2.0 Governing Policy/Procedure/Guideline

<u>Number/Name</u>	<u>Effective Date</u>
8.1 Password Policies for Electronic Systems	April 26, 2005
8.1 S Password Standards for Electronic Systems	August 2, 2005

### 3.0 Guidelines

The specifics of password requirements can not be published as it would compromise the effectiveness of the password. This leads to user frustration as the system rejects your proposed passwords. This document is available to guide you through the process of selecting a password that will meet the requirements without specifically disclosing the requirements.

A favorite technique of a hacker is to try to gain access to a system by breaking the ID/Password combination, using the access to retrieve vital information or to gain access to additional accounts. These attempts are usually automated processes that occur rapidly and never get tired of trying to guess the password.

Please refer to the Password Policy and Password Standards to obtain more information associated with your responsibilities as a password recipient.

#### 3.1 Approved Password Creation Methods:

- Choose a password of eight (8) or more characters
- Choose a password that contains a combination of these:
  - a-z
  - A-Z
  - 0-9
  - @ # % \_ - + = : , .
- Choose a password with at least one (1) digit
- Choose a password that does not need to be written down to remember
- Choose a password that can be typed quickly (especially if account is used in public access areas like labs or public access terminals)

### 3.2 Password Creation Methods to Avoid:

- Choosing a password that includes the tilde (~)
- Choosing a password that includes a blank space.
- Choosing a password that includes a dollar sign (\$).
- Choosing a password that includes an ampersand (&).
- Choosing a password that has the username in any format (including: reverse, capitalized or doubled).
- Choosing a password that has proper names (including: relatives and geographical locations).
- Choosing a password that has information about yourself (including: social security number, birth date, phone number and the street you live on).
- Choosing a password that appears in a dictionary (including: foreign and slang words should not be used).
- Choosing a password that has title of movies, books, compositions.
- Choosing a password that has any mythological or fictional character or race.
- Choosing a password that result from patterns on the keyboard.
- Choosing a password that has many repeating characters.
- Choosing a password that you have used previously.
- Choosing a password by applying a simple algorithm against previous passwords.
  - Backwards
  - Substituting number for vowels, R1ch2rd for Richard
  - Common substitutions for letters, 3 for e such as mov3
  - Appending or prefixing digits, apple234, 234pie
  - Incrementing digits
  - Appending or prefixing special characters

### 3.3 Methods to improve remembering passwords :

- Choose two easy to remember words that have no relation and separate them with a digit (examples: doG33soDa, boat9cAtch, fUdge15GooD)
- Choose a line from a poem or song and use just the first characters or a mixture of characters (example: 'To be or not to be' becomes toborn2b or tbORn0t2b or even twobornot2b)
- Use the new password immediately. Log out and log back in.
- After ten minutes, log out and log back in.
- Don't change your password just before leaving for a weekend or an extended period of time.
- Plan ahead. Make sure that changing a password will not be required at a critical time.

## 4.0 Responsibility for Implementation

ICT Director of IT Security Administration and ICT Director IT, Network and Systems.

## 5.0 Definitions

<u>Term</u>	<u>Definition</u>
<b>Brute Force Attack</b>	A method of defeating a cryptographic scheme by trying a large number of possibilities.

**6.0 Revision History**

<u>Requestor</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Putney	Draft 1 Password Guidelines	June 23, 2005	
Putney	Draft 2 Password Guidelines	July 21, 2005	
Dorendorf	Added information	July 28, 2005	August 2, 2005
Laundra	Copyedited/proofed for upload	August 18, 2005	